

**EXHIBIT H**

Washington, D.C.

April 13, 2020

# FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic

Fraudsters are leveraging increased fear and uncertainty during the COVID-19 pandemic to steal your money and launder it through the complex cryptocurrency ecosystem.

People of all ages, including the elderly, are being victimized by criminals through cryptocurrency-related fraud schemes. Developments in cryptocurrency technology and an increasing number of businesses accepting it as payment have driven the growing popularity and accessibility of cryptocurrency. There are not only numerous virtual asset service providers online but also thousands of cryptocurrency kiosks located throughout the world which are exploited by criminals to facilitate their schemes. Many traditional financial crimes and money laundering schemes are now orchestrated via cryptocurrencies.

The FBI advises you to be on the lookout for an increase in the following cryptocurrency fraud schemes related to COVID-19:

**Blackmail Attempts.** Threatening emails or letters in which scammers claim to have access to your personal information or knowledge of your "dirty secrets" and demand payment in Bitcoin to prevent release of this information have been circulating for years. With the advent of COVID-19, there is a new twist on this scam. The correspondence claims that the writer will both release your information and infect you and/or your family with coronavirus unless payment is sent to a Bitcoin wallet.

**Work from Home Scams.** Scammers, posing as employers, may ask you to accept a "donation" of funds into your own bank account and to deposit them into a crypto kiosk. The so-called "donation" is likely money stolen from others. Your acceptance and transfer of the stolen money is considered illegal money mule activity and potentially unlicensed money transmission.

**Paying for Non-Existent Treatments or Equipment.** Scammers have been known to lure customers from trusted e-commerce sites offering products that claim to prevent COVID-19 onto unrelated and unregulated messaging sites to accept payment in cryptocurrencies for products that do not actually exist.

**Investment Scams.** Criminals often pitch fraudulent investments in a "new" and developing cryptocurrency, such as an initial coin offering (ICO) or other investment vehicle to take a victim's money. These scams typically involve scenarios that seem "too good to be true"—offering large monetary returns for a short-term, small investment. The reality is that scammers steal the investment money for personal use and utilize the complexities of cryptocurrency to hide the true destination of the stolen funds.

Although there are legitimate charities, investment platforms, and e-commerce sites that accept payment in cryptocurrency, pressure to use a virtual currency should be considered a significant red flag.

By remembering the following tips regarding finances and cryptocurrency, you can better protect yourself from fraud:

- Verify that a vendor/charity is legitimate and accepts cryptocurrency before sending payments/donations.
- Conduct extensive research on potential investment opportunities.
- Do not use your personal bank accounts for work-from-home business-related activity or provide your bank account information to someone who is not named on the account.
- Contact law enforcement before paying out blackmail and/or extortion attempts and before converting your money into cryptocurrency to pay them.

The FBI's Criminal Investigative Division has an entire team dedicated to preventing and combating cryptocurrency money laundering and frauds. If you believe you are the victim of a fraud, or if you want to report suspicious activity, please contact your local field office or visit the FBI's Internet Crime Complaint Center at ic3.gov.

For accurate and up-to-date information about COVID-19, visit:

- coronavirus.gov
- cdc.gov/coronavirus
- usa.gov/coronavirus
- fbi.gov/coronavirus
- justice.gov/coronavirus

Most Wanted	News	What We Investigate	Contact Us
Ten Most Wanted	Stories	Terrorism	Field Offices
Fugitives	Videos	Counterintelligence	FBI Headquarters
Terrorism	Press Releases	Cyber Crime	Overseas Offices
Kidnappings / Missing Persons	Speeches	Public Corruption	
Seeking Information	Testimony	Civil Rights	Additional Resources
Bank Robbers	Podcasts and Radio	Organized Crime	Accessibility
ECAP	Photos	White-Collar Crime	eRulemaking
VICAP	Español	Violent Crime	Freedom of Information / Privacy Act
	Apps	WMD	Legal Notices
FBI Jobs			Legal Policies & Disclaimers
Submit a Tip	How We Can Help You	About	Privacy Policy
Crime Statistics	Law Enforcement	Mission & Priorities	USA.gov
History	Victims	Leadership & Structure	White House
FOIPA	Parents and Caregivers	Partnerships	No FEAR Act
Scams & Safety	Students	Community Outreach	Equal Opportunity
FBI Kids	Businesses	FAQs	
FBI Tour	Safety Resources		
	Need an FBI Service or More Information?		

